THE STRUCTURE AND APPLICATIONS OF GALOIS ALGEBRAS

Thomas Francis Noonan

United States
Naval Postgraduate School

THESIS

THE STRUCTURE AND APPLICATIONS
OF GALOIS ALGEBRAS

by

Thomas Francis Noonan

Thesis Advisor: D. L. Davis

June 1971

The Structure and Applications of Galois Algebras

by

Thomas Francis Noonan
Ensign, United States Navy
B.S., United States Naval Academy, 1970

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE
(with major in Mathematics)

from the

NAVAL POSTGRADUATE SCHOOL
June 1971

ABSTRACT

In this thesis we will construct a general Galois algebra and study its structure and ideals. After considering an example, we will look at some applications of Galois algebras. Then we will study one of the applications in more detail.

TABLE OF CONTENTS

I. INTRODUCTION

In this paper we shall discuss Galois algebras. We will begin by studying the general structure of a Galois algebra. Then we will attempt to prove some theorems concerning some of the properties of these algebras. After considering an example we will look into some of the uses which can be made of Galois algebras. A particular type of Galois algebra which is useful in the study of group algebras will then by studied more fully.

II. GENERAL STRUCTURE OF A GALOIS ALGEBRA

We will begin by constructing a Galois algebra. We shall make use of the symbol F_p to designate a finite field with p elements, and the symbol $F_p[x]$ to denote the ring of polynomials in the indeterminate, x, with coefficients in F. It is well known that $F_p[x]$ is a Euclidean domain. Hence, $F_p[x]$ is a principle ideal domain (see 1, Pg. 117). Consider f(x) an element of $F_p[x]$ and let $\langle f(x) \rangle$ be the ideal generated by f(x) in $F_p[x]$. Now consider the quotient ring $F_p[x]/\langle f(x) \rangle$.

Elements of the quotient ring are of the form $a(x)+\langle f(x) \rangle$, where a(x) is an element of $F_p[x]$. The elements of the quotient ring are added and multiplied by the following rules.

$$(a(x)+\langle f(x) \rangle)+(b(x)+\langle f(x) \rangle) = (a(x)+b(x)+\langle f(x) \rangle)$$

$$(a(x)+\langle f(x) \rangle)\ (b(x)+\langle f(x) \rangle) = (a(x)b(x)+\langle f(x) \rangle)$$

In $F_p[x] / \langle f(x) \rangle$, two elements, $a(x)+\langle f(x) \rangle$ and $b(x)+\langle f(x) \rangle$, are equal if and only if $a(x)-b(x)=c(x)f(x)$ for some $c(x)$ in $F_p[x]$. The quotient ring is also an algebra. This type of algebra is called a Galois algebra. The following general theorem will help us a great deal in studying this algebra.

A. THEOREM 1:

Let R be a principle ideal ring and let I be an ideal in R. Then the quotient ring, R/I, is a principle ideal ring.

Proof: Let J be an ideal in R/I. It follows that $J=\{k+I \mid k \in K\}$ where K is contained in R and $K=\bigcup J$. Because J is an ideal we know the following. If k_i+I and k_j+I are elements of J, then $(k_i+I)+(k_j+I)=(k_i+k_j+I)$ is an element of J. Therefore k_i+k_j is an element of K. Also $(k_i+I)(k_j+I)=(k_ik_j+I)$ is an element of J, which implies that k_ik_j is an element of K. The set $\{a(k+I) \mid k \in K,\ a \in R/I\}$ is contained in J which implies that RK is contained in K. Hence, it follows that K is an ideal in R. R is a principle ideal ring, therefore $K=\langle k \rangle$ for some k in R. Let $J'=\langle k+I \rangle$ where $K=\langle k \rangle$. Certainly J' is contained in J since k+I is an element of J. Let k_i+I be an arbitrary element of J. Therefore k_i is in K, which implies that $k_i=tk$ for some t in R. $k_i+I=tk+I=(t+I)(k+I)$ which is in J'. Therefore J is contained in J' which implies that $J=J'$. Therefore we have that R/I is a principle ideal ring.

From Theorem 1 we can easily conclude that $F_p[x]/\langle f(x)\rangle$ is a principle ideal ring. Therefore every ideal in a Galois algebra is principle.

We will now look at two theorems which will give us a better insight into the ideal structure of the Galois algebra $F_p[x]/\langle f(x)\rangle$.

B. THEOREM 2:

Let f(x) be an element of $F_p[x]$ and $\tilde{x} = x + \langle f(x)\rangle$. If $\langle g(\tilde{x})\rangle$ is any non-zero ideal in $F_p[x]/\langle f(x)\rangle$, then there exists a unique factor $g'(x)$ of f(x) such that $\langle g(\tilde{x})\rangle = \langle g'(\tilde{x})\rangle$.

Proof: $g(x) = \sum a_i x^i$, a_i elements of F.

$g(\tilde{x}) = g(x + \langle f(x)\rangle) = \sum a_i(\tilde{x})^i = \sum a_i(x^i + \langle f(x)\rangle)$

$= \sum a_i x^i + \langle f(x)\rangle = g(x) + \langle f(x)\rangle$

We know that $F_p[x]$ is a unique factorization domain (see 1, Pg. 117). Let $g'(x)$ be the greatest common divisor of $\{f(x), g(x)\}$. It follows that $g'(x) = k(x)f(x) + l(x)g(x)$ for some k(x), l(x) in $F_p[x]$.

$\Rightarrow g'(\tilde{x}) = g'(x) + \langle f(x)\rangle = l(x)g(x) + \langle f(x)\rangle = (l(x) + \langle f(x)\rangle)(g(x) + \langle f(x)\rangle)$

$\Rightarrow g'(\tilde{x}) \in \langle g(x) + \langle f(x)\rangle\rangle$

$\Rightarrow \langle g'(\tilde{x})\rangle \subseteq \langle g(\tilde{x})\rangle$. We now must show that $\langle g(\tilde{x})\rangle \subseteq \langle g'(\tilde{x})\rangle$. Let $a \mid b$ mean that a divides b. $g'(x) \mid g(x) \Rightarrow g'(x)h(x) = g(x)$ for some h(x) in $F_p[x]$. $g(\tilde{x}) = g(x) + \langle f(x)\rangle$

$= g'(x)h(x) + \langle f(x)\rangle = (g'(x) + \langle f(x)\rangle)(h(x) + \langle f(x)\rangle) \in \langle g'(\tilde{x})\rangle$

$\Rightarrow \langle g(\tilde{x})\rangle \subseteq \langle g'(\tilde{x})\rangle$. Therefore $\langle g(\tilde{x})\rangle = \langle g'(\tilde{x})\rangle$.

To complete the proof it must be shown that $g'(x)$ is unique. Suppose there exists an element $w(x)$ in $F_p[x]$ such that $w(x) \mid f(x)$ and $\langle w(\tilde{x})\rangle = \langle g(\tilde{x})\rangle$.

$\Rightarrow \langle w(\tilde{x})\rangle = \langle g'(\tilde{x})\rangle$

$\Rightarrow w(x) + \langle f(x)\rangle \in \langle g'(\tilde{x})\rangle$

$\Rightarrow w(x) + f(x) = t(x)g'(x) + \langle f(x)\rangle$ for some $t(x) \in F_p[x]$.

$\Rightarrow w(x) + h_1(x)f(x) = t(x)g'(x) + h_2(x)f(x)$ for some $h_1(x)$, $h_2(x) \in F_p[x]$.

$\Rightarrow w(x) = g'(x)t(x) + h_2(x)f(x) - h_1(x)f(x)$, but $g'(x) \mid f(x)$

$\Rightarrow f(x) = g'(x)p(x)$ for some $p(x)$ in $F_p[x]$.

$\Rightarrow w(x) = g'(x)t(x) + h_2(x)g'(x)p(x) - h_1(x)g'(x)p(x)$

$\Rightarrow w(x) = g'(x)\left[t(x) + h_2(x)p(x) - h_1(x)p(x)\right]$

$\Rightarrow g'(x) \mid w(x)$. We may use this same argument replacing $w(x)$ by $g'(x)$ and $g'(x)$ by $w(x)$ to show that $w(x) \mid g(x)$. It then follows that $g'(x) = w(x)$ and the proof is complete.

Note that an ideal in a Galois algebra is a subring and in fact a subalgebra. We therefore may consider the dimension of an ideal as a vector subspace.

C. THEOREM 3:

Let $f(x)$ be in $F_p[x]$ and $g(x) \in F_p[x]$ such that $g(x) \mid f(x)$. Then the dimension of the ideal $\langle g(\tilde{x})\rangle$ is the degree of $f(x)$ minus the degree of $g(x)$.

Proof: Let $\left| g(x) \right|$ denote the degree of $g(x)$.

$g(x) \mid f(x) \Rightarrow g(x)p(x) = f(x)$ for some $p(x)$ in $F_p[x]$.

$\Rightarrow |g(x)| \leq |f(x)|$. Let $k = |p(x)| = |f(x)| - |g(x)|$. Consider $\{ x^i g(x) + \langle f(x) \rangle \mid i = 0, \ldots, k-1 \}$. We will denote this set B, and we will show that B forms a basis for the ideal $\langle g(\tilde{x}) \rangle$. Let y be an element of $\langle g(\tilde{x}) \rangle \Rightarrow y = h(x)g(x) + \langle f(x) \rangle$ for some h(x) in $F_p[x]$. Suppose that $|h(x)| < k$.

$$\Rightarrow \sum_{i=0}^{s<k} a_i k^i = h(x) \Rightarrow y = \sum_{i=0}^{s<k} a_i x^i g(x) + \langle f(x) \rangle$$

$\Rightarrow y \in$ span of B. Suppose $|h(x)| \geq k \Rightarrow |h(x)| \, |g(x)| \geq |f(x)|$. Now apply the division algorithm to obtain $h(x) = t(x)f(x) + S(x)$ where $|S(x)| < k$. It follows that $h(x)g(x) = S'(x) + t'(x)f(x)$ where $|S'(x)| < |f(x)|$, and $S'(x) = S(x)g(x)$. It follows that $h(x)g(x)$

$$= \sum_{i=0}^{s<k} a_i x^i g(x) + \langle f(x) \rangle \Rightarrow y \in \text{Span B}.$$ We know that $\langle g(\tilde{x}) \rangle =$ Span of B. We must show, however, that the elements of B are independent to show that it is a basis for $\langle g(\tilde{x}) \rangle$. Suppose the elements of B are not linearly independent. Assume

$$\sum_{i=0}^{k-1} a_i x^i g(x) + \langle f(x) \rangle = 0 \text{ for } a_i,\ i = 0, \ldots, k-1 \text{ not all zero}$$

$$\Rightarrow \sum_{i=0}^{k-1} a_i x^i g(x) \in \langle f(x) \rangle$$

$$\Rightarrow f(x) \left| \sum_{i=0}^{k-1} a_i x^i g(x) \right. \Rightarrow |f(x)| \leq \left| \sum_{i=0}^{k-1} a_i x^i g(x) \right|$$

$\Rightarrow |f(x)| \leq k-1 + |g(x)| < k + |g(x)| = |f(x)|$. This is a contradiction.

Therefore the elements of B are independent, which implies that B is a basis for $\langle g(\tilde{x})\rangle$. Hence the dimension of $\langle g(\tilde{x})\rangle$ equals the order of the set B, which is k.

As a consequence of these last two theorems, we can see that the ideal structure of the algebra depends directly on the factorization of f(x) in $F_p[x]$. We therefore will study this factorization further. Assume that f(x) reduces into n factors which are powers of irreducible elements in $F_p[x]$. That is $f(x)=f_1(x)f_2(x)\ldots f_n(x)$, where $f_i(x)=p_i(x)^{k_i}$ and each $p_i(x)$ is an irreducible in $F_p[x]$ and each k_i is a finite positive integer, $i=1,\ldots,n$.

We will now define a new element of $F_p[x]$. Let $\overline{f_i(x)}$ denote f(x) divided by $f_i(x)$. It is then easily seen that the g. c. d. $\left\{\overline{f_1(x)}, \overline{f_2(x)},\ldots, \overline{f_n(x)}\right\}$ is the identity, which we shall denote by 1.

Consider the ideal generated by the set $\left\{\overline{f_1(x)}, \overline{f_2(x)},\ldots, \overline{f_n(x)}\right\}$. This is an ideal in $F_p[x]$. It is therefore principle. Let u(x) in $F_p[x]$ be the generator of the ideal. Since 1 is the g. c. d. $\left\{\overline{f_1(x)},\ldots, \overline{f_n(x)}\right\}$, $1=u(x)$. Therefore 1 is contained in $\left\langle\left\{\overline{f_1(x)},\ldots, \overline{f_n(x)}\right\}\right\rangle$. It follows that we may write 1 as the sum of elements in the ideal.

$1=t_1(x)\overline{f_1(x)}+t_2(x)\overline{f_2(x)}+\ldots+t_n(x)\overline{f_n(x)}$ for some $t_i(x)$, $i=1,\ldots,n$ in $F_p[x]$.

Let $e_i(x)=t_i(x)\overline{f_i(x)}$. Therefore $e_i(x)+\ldots+e_n(x)=1$. In $F_p[x]/\langle f(x)\rangle$ the identity element for multiplication is $1+\langle f(x)\rangle$ where 1 is the identity in $F_p[x]$.

Let us now consider the product $e_i(\tilde{x})e_j(\tilde{x})$.

$e_i(\tilde{x})=t_i(\tilde{x})\,\overline{f_i(\tilde{x})}$, $e_j(\tilde{x})=t_j(\tilde{x})\,\overline{f_j(\tilde{x})}$

$\Rightarrow e_i(\tilde{x})e_j(\tilde{x})=t_i(\tilde{x})\,t_j(\tilde{x})\,\overline{f_i(\tilde{x})}\,\overline{f_j(\tilde{x})}$, if $i\neq j$

$\Rightarrow \overline{f_i(x)}\,\overline{f_j(x)}=a(x)f(x)$ for some $a(x)\in F[x]$.

$\Rightarrow e_i(x)e_j(x)=b(x)f(x)$ where $b(x)=t_i(x)t_j(x)a(x)$

$\Rightarrow e_i(x)e_j(x)\in\langle f(x)\rangle\Rightarrow e_i(\tilde{x})e_j(\tilde{x})=0$.

We know that $e_1(\tilde{x})+e_2(\tilde{x})+\ldots+e_n(\tilde{x})=1$. Therefore

$e_i(\tilde{x})\left[e_1(\tilde{x})+\ldots+e_n(\tilde{x})\right]=e_i(\tilde{x})\,1=e_i(\tilde{x})$.

$\Rightarrow e_i(\tilde{x})e_1(\tilde{x})+\ldots+e_i(\tilde{x})e_i(\tilde{x})+\ldots+e_i(\tilde{x})e_n(\tilde{x})=e_i(\tilde{x})$

$\Rightarrow 0+\ldots+0+e_i(\tilde{x})^2+0+\ldots+0=e_i(\tilde{x})$

$\Rightarrow e_i(\tilde{x})^2=e_i(\tilde{x})$

In general $e_i(\tilde{x})e_j(\tilde{x})=\delta_{ij}e_i(\tilde{x})$, where δ_{ij} is the Kronecker delta function. Hence the $e_i(\tilde{x})$, $i=1,\ldots,n$ are orthogonal idempotents in $F[x]/\langle f(x)\rangle$.

Let $k(\tilde{x})$ be an element of $F[x]/\langle f(x)\rangle$. Then $k(\tilde{x})=k(\tilde{x})\,1=k(\tilde{x})\left[e_1(\tilde{x})+e_2(\tilde{x})+\ldots+e_n(\tilde{x})\right]=k(\tilde{x})e_1(\tilde{x})+\ldots+k(\tilde{x})e_n(\tilde{x})$. It follows then that every element of $F_p[x]/\langle f(x)\rangle$ can be represented as the sum of elements in the ideals $\langle e_i(\tilde{x})\rangle$. We would like to show that this representation is unique. To do this we need only show that the representation of the zero element in $F_p[x]/\langle f(x)\rangle$ is unique. Let $0=h_1(\tilde{x})e_1(\tilde{x})+h_2(\tilde{x})e_2(\tilde{x})+\ldots+h_n(\tilde{x})e_n(\tilde{x})$, where $h_i(x)$, $i=1,\ldots,n$, are elements of $F_p[x]/\langle f(x)\rangle$. Multiply each side by $e_1(\tilde{x})$. The result is that $h_1(\tilde{x})e_1(\tilde{x})=0$. Similarly, we may multiply by each $e_i(\tilde{x})$, $i=2,\ldots,n$. The result is that the only representation for 0 is $0+0+\ldots+0$. It

now follows that the representation of any element in the algebra is unique. The Galois algebra has therefore been shown to be the direct sum of the ideals $\langle e_i(\tilde{x})\rangle$.

We have reduced the study of a Galois algebra to the study of the ideals, $\langle e_i(\tilde{x})\rangle$, generated by the orthogonal idempotents. We will now consider some theorems concerning these ideals.

D. THEOREM 4:

Let I be an ideal in $F_p[x]/\langle f(x)\rangle$. Given any t an element in I, $t=u_1+\ldots+u_n$ where $u_i\in\langle e_i(\tilde{x})\rangle$. Define $U_i=\left\{u_i \,\middle|\, u_i\in\langle e_i(\tilde{x})\rangle \text{ and } u_i \text{ is a component of t for some t in I}\right\}$. Then U_i is an ideal in $\langle e_i(\tilde{x})\rangle$.

Proof: Suppose u, u' are elements of U_i for some i. Then there exists elements $g(\tilde{x})$ and $h(\tilde{x})$ in $F_p[x]/\langle f(x)\rangle$ such that

$g(\tilde{x})=g(\tilde{x})e_1(\tilde{x})\oplus\ldots\oplus u\oplus\ldots\oplus g(\tilde{x})e_n(\tilde{x})$

$h(\tilde{x})=h(\tilde{x})e_1(\tilde{x})+\ldots+u'+\ldots+h(\tilde{x})e_n(\tilde{x})$

$\Rightarrow h(\tilde{x})+g(\tilde{x})=(h(\tilde{x})+g(\tilde{x}))e_1(\tilde{x})+\ldots+u+u'+\ldots+(h(\tilde{x})+g(\tilde{x}))e_n(\tilde{x})$

$h(\tilde{x})+g(\tilde{x})$ is in $I\Rightarrow u+u'\in U_i$. This same type of argument holds for $uu'\in U_i$, when $h(\tilde{x})$ and $g(\tilde{x})$ are multiplied. Let $v\in e_i(\tilde{x})$. It follows there exists a $q(x)$ in $F_p[x]/\langle f(x)\rangle$ such that

$q(\tilde{x})=q(\tilde{x})e_1(\tilde{x})+\ldots+v+\ldots+q(\tilde{x})e_n$. Let u and $g(\tilde{x})$ be defined as above. $q(\tilde{x})g(\tilde{x})$ is in $I\Rightarrow uv$ is in U_i. It then follows that U_i is an ideal in $\langle e_i(\tilde{x})\rangle$.

Next we prove a theorem which will give us a better idea of the structure of the algebra.

E. THEOREM 5:

$F_p[x]/\langle f_i(x)\rangle$ is isomorphic to $\langle e_i(\tilde{x})\rangle$.

Proof: Let $h(x)+\langle f_i(x)\rangle$ be an element of $F_p[x]/\langle f_i(x)\rangle$. Define the mapping $T: F_p[x]/\langle f_i(x)\rangle \rightarrow \langle e_i(\tilde{x})\rangle$ by $T(h(x)+\langle f_i(x)\rangle) = h(x)e_i(x)+\langle f(x)\rangle$. This certainly defines a homomorphism. Suppose that $T(h_1(x)+\langle f_i(x)\rangle) = T(h_2(x)+\langle f(x)\rangle)$

$\Rightarrow h_1(x)e_i(x)+\langle f(x)\rangle = h_2(x)e_i(x)+\langle f(x)\rangle$. Let $h_1(x)e_i(x)+b_1(x)f(x)$ be an element of $h_1(x)e_i(x)+\langle f(x)\rangle$

$\Rightarrow$There exists a $b_2(x)$ such that $h_1(x)e_i(x)+b_1(x)f(x) = h_2(x)e_i(x)+b_2(x)f(x)$.

$\Rightarrow (h_1(x)-h_2(x))\, e_i(x) = b_3(x)f(x)$ where $b_3(x) = b_2(x)-b_1(x)$.

$e_i(x) = l_i(x)\, \overline{f_i(x)}$

$\Rightarrow (h_1(x)-h_2(x))t_i(x) = b_3(x)f_i(x)$. $f_i(x) = p_i(x)^{k_i} \Rightarrow$

$p_i(x)^{k_i} \mid (h_1(x)-h_2(x))t_i(x)$. This gives us three cases. Either $p_i(x)^{k_i} \mid (h_1(x)-h_2(x))$ or $p_i(x)^{k_i} \mid t_i(x)$ or $p_i(x)$ divides both $(h_1(x)-h_2(x))$ and $t_i(x)$.

Suppose $p_i(x) \mid t_i(x) \Rightarrow p_i(x) \mid e_i(x)$. We know that $p_i(x)$ divides $e_j(x)$ $j=1, \ldots, i-1, i+1, \ldots, n \Rightarrow p_i(x) \mid e_1(x)+\ldots+e_n(x) \Rightarrow$

$p_i(x) \mid 1 \Rightarrow p_i(x) = 1 \Rightarrow f_i(x) = 1$. $\Rightarrow 1$ is an element of $\langle f_i(x)\rangle \Rightarrow$

$F_p[x]/\langle f_i(x)\rangle$ has only one element, namely, $0+\langle f_i(x)\rangle$. But since $f_i(x) \mid e_i(x) \Rightarrow f(x) \mid e_i(x) \Rightarrow e_i(x)$ is an element of $\langle f(x)\rangle \Rightarrow \langle e_i(\tilde{x})\rangle$ has

only the zero element, $0+\langle f(x)\rangle$. Therefore T is an isomorphism. This takes care of the case that $p_i(x)^{k_i} \mid t_i(x)$ and the case that $p_i(x)$ divides both $t_i(x)$ and $(h_1(x)-h_2(x))$.

Now consider the remaining case $p_i(x)^{k_i} \mid (h_1(x)-h_2(x))$ $\Rightarrow f_i(x) \mid (h_1(x)-h_2(x))$. But by our previous definition this means that $h_1(x)$ is equal to $h_2(x)$ in $F_p[x]/\langle f_i(x)\rangle$. T is a 1-1 homomorphism. T is onto since $h(x)e_i(x)+\langle f(x)\rangle$ in $\langle e_i(\tilde{x})\rangle$ has $h(x)+\langle f(x)\rangle$ in $F_p[x]/\langle f_i(x)\rangle$ as its preimage. Therefore T is an isomorphism.

We therefore know that the Galois algebra $F_p[x]/\langle f(x)\rangle$ is isomorphic to $F_p[x]/\langle f_1(x)\rangle \oplus \ldots \oplus F_p[x]/\langle f_n(x)\rangle$. This tells us a great deal about the structure of the algebra and its ideals. Combining theorem 4 and theorem 5 we see that every ideal in $F_p[x]/\langle f(x)\rangle$ splits into the direct sum of ideals in $\langle e_i(\tilde{x})\rangle$. These ideals in $\langle e_i(\tilde{x})\rangle$ are isomorphic to ideals in $F_p[x]/\langle f_i(x)\rangle$. From theorem 2 we may assume that these ideals are generated by factors of $f_i(x)$. We know, however, that the only factors of $f_i(x)$ are $p_i(x)^j$, $j=0, \ldots, k_i$. Therefore the complete decomposition of an ideal in $F_p[x]/\langle f(x)\rangle$ is known.

Our next step will be to consider an example.

III. AN EXAMPLE OF A GALOIS ALGEBRA

In this example we will set our field F equal to F_2, the field of two elements. We will take $x^9+x^8+x^6+x^5+x^4+x^3+x+1$ to be our polynomial f(x) in $F_p[x]$. We can prove that f(x) factors into $f_1(x)f_2(x)$, where $f_1(x)=p_1(x)$, $f_2(x)=p_2(x)^2$. The polynomials $p_i(x)$ are $p_1(x)=x^3+x^2+1$, $p_2(x)=x^3+x+1$. We see that $\overline{f_1(x)}=(x^3+x+1)^2$ and $\overline{f_2(x)}=(x^3+x^2+1)$. From previous results it is known that $t_1(x)\ (x^3+x+1)^2\ t_2(x)\ (x^3+x^2+1)=1$, for some $t_1(x)$, $t_2(x)$ in $F_2[x]$. Using the Euclidean algorithm we find $t_1(x)=x^2$ and $t_2(x)=x^5+x^4+x^3+1$. This result can easily be verified.

$$(x^5+x^4+x^3+1)(x^3+x^2+1)+x^2(x^6+x^2+1)$$

$$=(x^8+x^7+x^6+x^3+x^7+x^6+x^5+x^2+x^5+x^4+x^3+1)+(x^8+x^4+x^2)$$

$$=1 \text{ in } F_2[x].$$

Remember all operations in $F_2[x]$ are defined such that $x^i+x^i=0 \Rightarrow x^i=-x^i$.

It now follows that $e_1(x)=x^8+x^4+x^2+1$ and $e_2(x)=x^8+x^4+x^2$. It can easily be seen that $e_1(x)+e_2(x)=1$. Let us check, however, the formula $e_i(\tilde{x})e_j(\tilde{x})=\delta_{ij}e_i(\tilde{x})$.

$e_1(\tilde{x})e_1(\tilde{x}) = x^{16}+x^{12}+x^{10}+x^8+x^{12}+x^8+x^6+x^4+x^{10}+x^6+x^4+x^2+x^8$

$+x^4+x^2+1+\langle f(x)\rangle = x^{16}+x^8+x^4+1+\langle f(x)\rangle$

$= x^8+x^4+x^2+1+(x^{16}+x^2)+\langle f(x)\rangle$. We must show that $x^{16}+x^2$ is an element of $\langle f(x)\rangle$.

$$
\begin{array}{r}
x^7+x^6+x^5+x^2 \\
x^9+x^8+x^6+x^5+x^4+x^3+1 \;\overline{)\; x^{16}+x^2} \\
\underline{x^{16}+x^{15}+x^{13}+x^{12}+x^{11}+x^{10}+x^7} \\
x^{15}+x^{13}+x^{12}+x^{11}+x^{10}+x^7+x^2 \\
\underline{x^{15}+x^{14}+x^{12}+x^{11}+x^{10}+x^9+x^6} \\
x^{14}+x^{13}+x^9+x^7+x^6+x^2 \\
\underline{x^{14}+x^{13}+x^{11}+x^{10}+x^9+x^8+x^5} \\
x^{11}+x^{10}+x^8+x^7+x^6+x^5+x^2 \\
\underline{x^{11}+x^{10}+x^8+x^7+x^6+x^5+x^2} \\
0
\end{array}
$$

$\Rightarrow x^{16}+x^2 = (f(x))\ (x^7+x^6+x^5+x^2)$

$\Rightarrow e_1(\tilde{x})^2 = x^8+x^4+x^2+1+\langle f(x)\rangle = e_1(\tilde{x})$

$e_2(\tilde{x})e_2(\tilde{x}) = x^{16}+x^{12}+x^{10}+x^{12}+x^8+x^6+x^{10}+x^6+x^4+\langle f(x)\rangle$

$= x^{16}+x^8+x^4+\langle f(x)\rangle$

$= x^8+x^4+x^2+(x^{16}+x^2)+\langle f(x)\rangle$

$= x^8+x^4+x^2+\langle f(x)\rangle = e_2(\tilde{x})$

$e_1(\tilde{x})e_2(\tilde{x}) = x^{16}+x^{12}+x^{10}+x^8+x^{12}+x^8+x^6+x^4+x^{10}+x^6+x^4+x^2+\langle f(x)\rangle$

$= x^{16}+x^2+\langle f(x)\rangle$

$= \langle f(x)\rangle$

We have therefore verified the formula $e_i(\tilde{x})e_j(\tilde{x})=\delta_{ij}e_i(\tilde{x})$ for this example.

It follows from our previous theorems that $F_2[x]/f(x) = \langle x^8+x^4+x^2+1+\langle f(x)\rangle\rangle \oplus \langle x^8+x^4+x^2+\langle f(x)\rangle\rangle$, which is isomorphic to $F_2[x]/\langle x^3+x^2+1\rangle \oplus F_2[x]/\langle (x^3+x+1)^2\rangle$.

We will discuss now the usefulness of Galois algebras in the study of group algebras.

IV. GROUP ALGEBRAS

In this section we will consider only finite groups. Given a finite group G and a field F, the group algebra of G over F, which we shall denote by F[G], is the set of mappings from G to F. Let $G=\{g_1=0, g_2, \ldots, g_n\}$. We may then consider F[G] to be the collection of all $a_1g_1+\ldots+a_ng_n$ where a_i are elements of F. The elements of F[G] are added pointwise and multiplied using convolution. That is, for f, h in F[G], $fh(g_i)=\sum f(g_j)h(g_k)$ where the sum is taken over all pairs g_j, g_k in G such that $g_jg_k=g_i$.

We will now further limit our study to finite cyclic groups, that is, groups generated by a single element of finite order.

First we will show the relation between the group algebra of a finite cyclic group and a Galois albegra.

A. THEOREM 6:

Let G be a finite cyclic group of order n. Then F[G] is isomorphic to $F_p[x]/\langle x^n-1\rangle$.

Proof: Let I be the ideal $\langle x^n-1\rangle$ in $F_p[x]$. Define a mapping $S:F[G]\to F_p[x]/I$ by $S(a)=x+I$, where a is a generator of G, $S(1)=1+I$, where 1 is the identity in G. $S(a^2)=x^2+I, \ldots,$ $S(a^{n-1})=x^{n-1}+I$. This defines the mapping S on a basis for F[G].

Let t be an element of $F[G] \Rightarrow t=\sum_{i=0}^{n-1} \alpha_i a^i$, $\alpha_i \in F$. Therefore

$$S(t)=\sum_{i=0}^{n-1} \alpha_i x^i+I=\sum_{i=0}^{n-1} \alpha_i \tilde{x}^i$$

S defined as above is certainly a mapping and a homomorphism for addition. We will now consider multiplication.

$$\left(\sum_{i=0}^{n-1} \alpha_i a^i\right)\left(\sum_{i=0}^{n-1} \beta_i a^i\right)=\sum_{k=0}^{n-1} \alpha_k a^k \text{ where } \alpha_k=\sum \alpha_i \beta_j \text{ where } i+j\equiv k \bmod n.$$

$$S\left(\sum_{i=0}^{n-1} \alpha_i a^i\right)S\left(\sum_{i=0}^{n-1} \beta_i a^i\right)=\left(\sum_{i=0}^{n-1} \beta_i \tilde{x}^i\right)\left(\sum_{i=0}^{n-1} \alpha_i \tilde{x}^i\right)=\sum_{k=0}^{n-1} \gamma'_k \tilde{x}^k \text{ where } \gamma'_k=\sum \alpha_i \beta_j$$

such that $i+j=k \bmod n$. We therefore see that S is a homomorphism for multiplication too.

We would like to show that S is one-to-one. To do this we need only show that $s(t)=0$ implies $t=0$. Suppose $S(T)=0$, then

$\sum_{i=0}^{n-1} \alpha_i x^i=0 \Rightarrow \sum_{i=0}^{n-1} \alpha_i x^i$ is in I which implies that $x^n-1 \Big| \sum_{i=0}^{n-1} \alpha_i x^i$, but

$\Big|\sum_{i=0}^{n-1} \alpha_i x^i \leq n-1 \Rightarrow \sum_{i=0}^{n-1} \alpha_i x^i=0$. Therefore $\alpha_i=0$ which means that $t=0$. S is certainly a mapping onto $F_p[x]/I$, since S is linear and

it maps onto the set $\{1+I,\ x+I,\ \ldots,\ x^{n-1}+I\}$ which is a basis for $F_p[x]/I$. Therefore S is an isomorphism.

This isomorphism implies that the group algebra of a finite cyclic group over the field F has the same properties as the Galois algebra, $F_p[x]/\langle x^n-1\rangle$, where n is the order of the group. We know that $F_p[x]/\langle x^n-1\rangle$ can be represented as the direct product of some ideals in the algebra. This implies that the group algebra can be split similarly.

V. THE GALOIS ALGEBRA $F_p[x]/\langle x^n-1\rangle$

We have just seen how the study of a group algebra of a finite cyclic group relates to the study of the Galois algebra $F_p[x]/\langle x^n-1\rangle$. Because of the usefulness of this particular type of Galois algebra we will study it further in an attempt to learn more about the cyclic group algebra.

We know already that this algebra will split into the direct sum of other algebras which have as generators powers of some irreducibles in $F_p[x]$. We do not know, however, how many algebras $F_p[x]/\langle x^n-1\rangle$ splits into or in what order these algebras occur. We therefore must study the factorization of x^n-1 in $F_p[x]$.

We will first define a function $\emptyset$. Let $\emptyset(n)$ be the order of the set $\{a \mid a \in N,\ a<n,\ \text{and g. c. d. } (a, n)=1\}$ (see 2, Pg. 112). This function is

known as the Euler ϕ-function. We will also define a polynomial, $\Phi_n(x) = \prod_{\substack{0 \le k \le n \\ (k,n)=1}} (x - \xi^k)$, where ξ is a primitive nth root of unity (see 3, Pg. 231). The following useful lemma can now be proven.

A. LEMMA 1:

$\Phi_d(x) \in \mathbb{Z}(x)$ and $x^n - 1 = \prod_{d \mid n} \Phi_d(x)$.

A proof of this lemma may be found in Dean (3, Pg. 231).

The polynomials $\Phi_n(x)$ are called cyclotomic polynomials. It can be shown that these polynomials are irreducible over the ring of integers (see 2, Pg. 161). This, however, does not insure that the polynomials $\Phi_n(x)$ are irreducible over the finite field, F_p, being considered.

We will suppose that we are given the polynomial $x^n - 1$ and some finite field, F_p. If $p \mid n$ there exists an n' such that $\gcd(p, n') = 1$, and $p^i n' = n$ for some i. It follows that $(x^n - 1) \equiv (x^{n'} - 1)^{p^i} \bmod p$ (see 4, Pg. 95). Therefore if we know the factorization of $(x^{n'} - 1)$ we will know the complete factorization of $x^n - 1$. Without loss of generality we will assume that the $\gcd(p, n) = 1$.

We already have that $x^n - 1 = \prod_{d \mid n} \Phi_d(x)$. Let A_d be the multiplicative group of least positive residues mod d which are relatively prime to d. We then define B_d to be the quotient group $A_d / \langle p \rangle$, where $\langle p \rangle$ is

the subgroup of A_d generated by p mod d. Note gcd(p, d)=1. The elements of B_d are therefore cosets of the group A_d.

Let k be an element of B_d. We define $\psi_k(x) = \prod_{i \in k} (x - \xi_d^i)$, where ξ_d is a primitive dth root of unity. We now state an important lemma.

B. LEMMA 2:

$\psi_k(x) \in F_p[x]$ and $\Phi_d(x) = \prod_{k \in B_d} \psi_k(x)$ is the complete factorization of $\Phi_d(x)$ into irreducibles over $F_p[x]$.

The proof of this lemma requires some elements of Galois theory beyond the scope of this paper. For a proof see Davis (5).

Consider $\psi_k(x)$ the factors of a given $\Phi_d(x)$. Each k in B_d is a coset of the same order. Therefore each $\psi_k(x)$ is of the same degree. The order of the cosets is e, where e is the order of the ideal $\langle p \rangle$. The number of factors, $\psi_k(x)$, of $\Phi_d(x)$ is m, where m is the order of B_d. We can see that m equals the order of A_d divided by e. We know, however, that the order of A_d is $\phi(d)$. Therefore the number of irreducible factors of $\Phi_d(x)$ is precisely $\phi(d)$ divided by e. This tells us how $x^n - 1$ factors in F_p.

Note that if n is a prime the result is simplified.

$$x^n - 1 = \Phi_1(x)\Phi_n(x)$$

$$= (x-1) f_1(x) \ldots f_t(x)$$

where the polynomials $f_i(x)$ have the same degree and t equals $\phi(n)$ divided by the order of $\langle p \rangle$. F_p is the field over which we are working and $\langle p \rangle$ is in A_n. Note that $\phi(n) = n - 1$ since n is prime.

VI. EXAMPLE TWO

Suppose that we are given the polynomial $x^{15}-1$, and we would like to factor it over the field F_7.

$$x^{15}-1=\prod_{d\mid 15} \Phi_d(x)$$

We can easily see that $\Phi_1(x)=x-1$. We also know that $x^3-1=\Phi_1(x)\Phi_3(x)$. This implies that $\Phi_3(x)=x^2+x+1$.

$$x^5-1=\Phi_1(x)\Phi_5(x) \Rightarrow \Phi_5(x)=\frac{x^5-1}{x-1}=x^4+x^3+x^2+x+1$$

$$\Phi_{15}(x)=\frac{x^{15}-1}{(x^3-1)(x^4+x^3+x^2+x+1)} \Rightarrow$$

$$\Phi_{15}(x)=x^8-x^7+x^5-x^4+x^3-x+1$$

$$=x^8+6x^7+x^5+6x^4+x^3+6x+1 \mod 7$$

$A_3=\{1, 2\}$, $A_5=\{1, 2, 3, 4\}$, $A_{15}=\{1, 2, 4, 7, 8, 11, 13, 14\}$. We can now find $B_3=A_3/\langle 7\rangle=\{\{1\}, \{2\}\}$, $B_5=A_5/\langle 7\rangle=\{\{1, 2, 3, 4\}\}$, $B_{15}=A_{15}/\langle 7\rangle=\{\{7, 4, 13, 1\}, \{2, 8, 11, 14\}\}$. We can see that $\Phi_5(x)$ has only one factor. This means that $\Phi_5(x)$ is irreducible in $F_7[x]$. $\Phi_3(x)$ and $\Phi_{15}(x)$ each split into two factors. We have a formula to get these factors. This formula, however, in most cases is difficult to use. There are, though, tables which we may use. For this example we will use the tables by Church (4). To find the factors for $\Phi_{15}(x)$ we look under irreducible polynomials of degree four, modulo seven. We know that these polynomials will divide $x^{15}-1$ mod seven so they

must have an exponent of 15 or less. We find in the tables that there are two such polynomials which have an exponent of 15. They are $x^4+2x^3+4x^2+x+2$ and $x^4+4x^3+2x^2+x+4$. Using the same type of argument we find the factors of $\Phi_3(x)$ mod seven to be $x+5$ and $x+3$. Checking, we see

$$(x^4+2x^3+4x^2+x+2)(x^4+4x^3+2x^2+x+4)$$

$$= x^8+2x^7+4x^6+x^5+2x^4+4x^7+8x^6+16x^5+4x^4+8x^3+2x^6+4x^5+8x^4+2x^3$$

$$+4x^2+x^5+2x^4+4x^3+x^2+2x+4x^4+8x^3+16x^2+4x+8$$

$$= x^8+6x^7+x^5+6x^4+x^3+6x+1$$

$$= \Phi_{15}(x)$$

$$(x+5)(x+3) = x^2+8x+15 = x^2+x+1 = \Phi_3(x)$$

By our previous results we see that the group algebra of a cyclic group of order 15 over the field F_7 is isomorphic to $F_7[x]/\langle x-1\rangle \oplus F_7[x]/\langle x+5\rangle \oplus F_7[x]/\langle x^4+x^3+x^2+x+1\rangle \oplus F_7[x]/\langle x^4+2x^3+4x^2+x+2\rangle \oplus F_7[x]/\langle x^4+4x^3+2x^2+x+4\rangle$. We see that the group algebra splits into the direct sum of six fields. The first three fields are isomorphic to F_7. The last three are isomorphic to a field extension of dimension four over F_7.

VII. CONCLUSION

We have constructed and studied a general Galois algebra. The structure of the algebra and of its ideals has been determined. We have seen one of the uses of a Galois algebra in the study of group algebras. There are other applications of Galois algebras which we have not considered. One of these is in the study of factorization of polynomials into irreducibles over finite fields.

We would like to have been able to study Galois algebras of multi-variables. However, even in the relatively simple case of two variables this study proves very difficult. The main difficulty is that $F[x, y]$ is not a principle ideal domain.

BIBLIOGRAPHY

1. Herstein, I.N., Topics in Algebra, Blaisdell, 1964.

2. Van Der Waerden, B.L., Modern Algebra, Frederick Ungar Publishing Co., 1949.

3. Dean, Richard A., Elements of Abstract Algebra, Wiley, 1966.

4. Jacobson, Nathan, Lectures in Abstract Algebra Vol. II, D. Van Nostrand, 1964.

5. Davis, D.L., On the Distribution of the Signs of the Conjugates of the Cyclotomic Units in the Maximal Real Subfield of the qth Cyclotomic Field, q a Prime, Ph.D. Thesis, California Institute of Technology, 1969.

6. Church, Randolf, "Tables of Irreducible Polynomials for the First Four Prime Moduli", Annals of Mathematics, Vol. 36, No. 1, January 1935.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Documentation Center Cameron Station Alexandria, Virginia 22314	2
2.	Library, Code 0212 Naval Postgraduate School Monterey, California 93940	2
3.	Asst Professor D. L. Davis Mathematics Department Naval Postgraduate School Monterey, California 93940	1
4.	Ens. Tom Noonan, USN 2160 Sunnyview Drive Dubuque, Iowa 52001	1

Security Classification

DOCUMENT CONTROL DATA - R & D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY (Corporate author)	2a. REPORT SECURITY CLASSIFICATION
Naval Postgraduate School Monterey, California 93940	Unclassified
	2b. GROUP

3. REPORT TITLE

The Structure and Applications of Galois Algebras

4. DESCRIPTIVE NOTES (Type of report and, inclusive dates)

Master's Thesis; June 1971

5. AUTHOR(S) (First name, middle initial, last name)

Thomas F. Noonan

6. REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS
June 1971	27	6

8a. CONTRACT OR GRANT NO.	9a. ORIGINATOR'S REPORT NUMBER(S)
b. PROJECT NO.	
c.	9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report)
d.	

10. DISTRIBUTION STATEMENT

Approved for public release; distribution unlimited.

11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY
	Naval Postgraduate School Monterey, California 93940

13. ABSTRACT

In this thesis we will construct a general Galois algebra and study its structure and ideals. After considering an example, we will look at some applications of Galois algebras. Then we will study one of the applications in more detail.

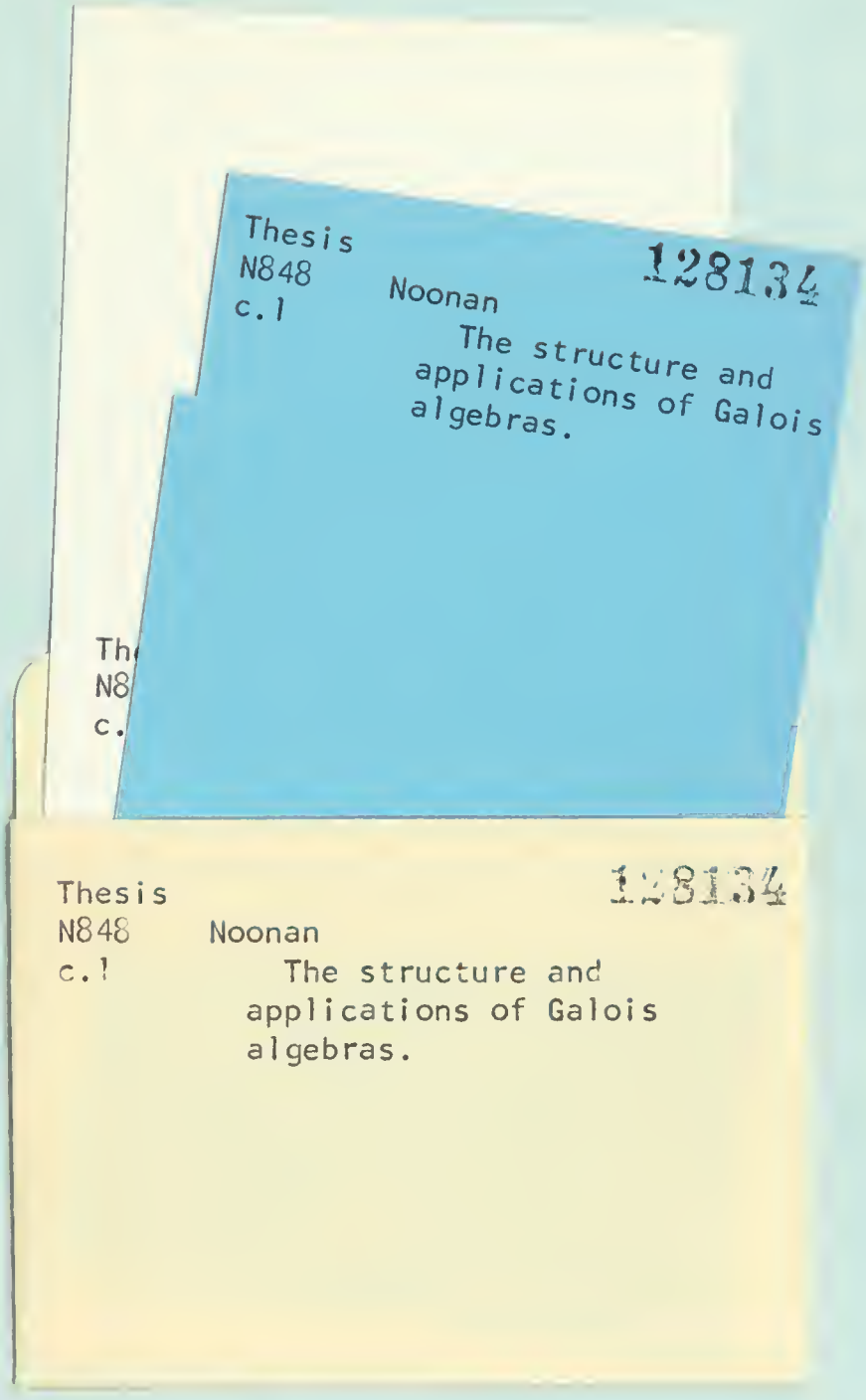
DD FORM 1 NOV 65 1473 (PAGE 1)

S/N 0101-807-6811

Security Classification

A-31408

KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
Algebra						
Galois Algebras						
Group Algebras						



Thesis
N848
c.1
128134
Noonan
The structure and applications of Galois algebras.